Call or Text: 720-731-3179
Email: Support@rmts-colorado.com
Website: www.rmts-colorado.com

Hardening the Homefront.

Home Network Hardening

1. Use Private Hardware: Replace ISP-provided routers with high-end, consumer-grade hardware (e.g., ASUS, Synology, or Ubiquiti) for greater security control.
2. Segment via VLANs: Create separate Wi-Fi networks for:
    a. Primary: Personal/Work laptops and phones.
    b. IoT: Cameras, smart speakers, and appliances.
    c. Guest: For visitors only.
3. Enable WPA3 Encryption: Use the strongest available encryption standard for wifi routers
4. Secure the Router Admin: Change default passwords and disable "Remote Management."
5. Audit Connected Devices: Remove or disable any devices that are no longer in use or lack modern security updates.

System Hardening

1. Update all computers and Devices
    a. Set a calendar reminder to perform updates and backups
2. Backup all systems at least quarterly
3. Anytime a new system is added to the home network complete an onboarding checklist
    a. Antivirus installed
    b. Browser Protection turned on
    c. Updated
    d. Change the system name to something recognizable

Identity & Accounts

1. MFA is no longer optional. Authenticator Apps are the best option (Google, Microsoft, etc)
2. Use a family Password Manager. Specifically with dark web monitoring to identify unsafe credentials
    a. Unique PWs for all accounts
    b. 17+ Characters
    c. Use passphrase generator for manual passwords
    d. Start using Passkeys whenever available
3. Scrub OSINT Data. Use third-party services to scrub as much family data from the web as possible. Family addresses, phone numbers, etc. (Services like Deleteme)
4. Map your digital footprint.
    a. You cannot defend what you cannot see
    b. For yourself, your spouse, your children

Call or Text: 720-731-3179
Email: Support@rmts-colorado.com
Website: www.rmts-colorado.com

Mobile & Travel Security

1. SIM Swap guards. Contact cellular carries to add "Port Out PINS or "SIM Locks" to all family phone lines
2. Disable Geotagging. Ensure "Location Services" for camera apps are off to prevent photos from revealing the home address.
3. VPN for Travel. Install a trusted VPN on all mobile devices for use on public wifi. (Airports, Hotels, Coffee Shops, etc)

Incident Response Plan

1. Have a family safe word to defend against deep fake audio and video scams.
2. Have a response card on the fridge or family facing.
    a. Who to call
    b. When to call
    c. How to report suspicious messages, texts, or activity
3. Encourage a family culture of security
    a. Reward reporting and taking secure actions.
    b. Make security a team sport – teaching good cyber safety lasts a lifetime.
4. Have professional help on standby. Like a good mechanic, dentist, and doctor. Having a cybersecurity professional that you can call is critical.

Reach out to our offices if you would like to discuss any of these measures in greater detail.
Our professional security consultants are always happy to help.